



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/567,752	02/10/2006	Paolo Abeni	099520022	5634
22852	7590	06/22/2009		
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP 901 NEW YORK AVENUE, NW WASHINGTON, DC 20001-4413			EXAMINER SIMS, JING F	
			ART UNIT 2437	PAPER NUMBER
			MAIL DATE 06/22/2009	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

# Office Action Summary

**Application No.**

10/567,752

**Applicant(s)**

ABENI, PAOLO

**Examiner**

JING SIMS

**Art Unit**

2437

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 10 February 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-50 is/are pending in the application.
- 4a) Of the above claim(s) 1-25 is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 26-50 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-893)
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date: \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_
- Paper No(s)/Mail Date 2/10/2006

### **DETAILED ACTION**

1. The instant application having Application No. 10/567,752 filed on 2/10/2006 is presented for examination by the examiner.

### ***Oath/Declaration***

2. The applicant's oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in **37 C.F.R. 1.63**.

### ***Priority***

3. As required by **M.P.E.P. 201.14(c)**, acknowledgement is made of applicant's claim for priority based on applications filed on 8/11/2003 (PCT/IT03/00505).

Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

### ***Drawings***

4. The drawings figure 1 to figure 5 are objected to because lacking of the description or content for the corresponding reference numbers. For example, reference numbers 12, 14, 16, 18 in figure 1, reference numbers 14, 16, 18 in figure 2, etc. Brief description of the corresponding reference numbers are needed in empty boxes.
5. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application.

Art Unit: 2437

Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

#### ***Information Disclosure Statement***

6. The information disclosure statement (IDS) submitted on 2/10/. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

#### ***Claim Rejections - 35 USC § 101***

7. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 26 is rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter. Although the preamble of the claim recites "an intrusion detection system", the body of the claim does not positively recite any elements of hardware. It discloses the intrusion detection system comprising a sniffer, a pattern machine engine and a response analysis engine. In light the specification, the three elements are not described or suggested as hardware; therefore, claim 1 has being directed to non-statutory subject matter.

Claims 27-37 are rejected under 35 U.S.C. 101 because they are depended on claim 1; however, they do not add any feature or subject matter that would solve any of the non-statutory deficiencies of the claim 1.

***Claim Rejections - 35 USC § 102***

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

9. **Claims 26-28, 30-32, 35-44, and 47-50 are rejected under 35 U.S.C. 102(a) as being anticipated by Lahtinen (European Publication no. EP 1330095 A1).**

**As per claim 26**, Lahtinen discloses an intrusion detection system for detecting unauthorised use of a network, comprising:

a sniffer for capturing data being transmitted on said network (*i.e.* [0014], *lines 31-33, monitoring process*) and a pattern matching engine receiving data captured by said sniffer and comparing said data with attack signatures (*i.e.* [0016], *matching the data stream against known misuse patterns*) for generating an event when a match between captured data and at least one attack signature is found (*i.e.* [0018], *generating an alarm event*); and

a response analysis engine, triggered by said event for comparing with response signatures the data being transmitted on said network as a response to said data matched with said attack signature and for correlating the results of said comparisons with attack and response signatures for generating an alarm (*i.e.* [0044], *analysis of response-request pairs, for example*).

**As per claims 27 and 40**, wherein said data being transmitted on said network as a response to said data matched with said attack signature is captured by said sniffer by performing an analysis of source IP address in data packets transmitted on said network (*i.e.* [0059], *parsed request and find IP address, for example*).

**As per claim 28**, the system of claim 26, wherein said data being transmitted on said network as a response to said data matched with said attack signature is captured by said sniffer by performing an analysis of both source and

Art Unit: 2437

destination IP addresses in data packets transmitted on said network (*i.e. page 3, [0009], IP frame on TCP packets, target and destination port, for example*).

**As per claims 30 and 42**, wherein said response analysis engine generates an alarm when said data being transmitted on said network as a response to said data matched with said attack signature indicates that a new network connection has been established (*i.e. [0044], the analysis of the response-request pairs*).

**As per claims 31 and 43**, the system of claim 26, wherein said response signatures are arranged in two categories, response signatures identifying an illicit traffic, and response signatures identifying legitimate traffic (*i.e. fig 7, configured states, and [0032], a table of available state, and legitimate/valid request, for example*).

**As per claim 32**, the system of claim 31, wherein said response analysis engine generates an alarm when a match between captured data and a response signature identifying illicit traffic is found (*i.e. [0008], generates an alarm when something suspicious is detected in traffic*).

**As per claim 35**, the system of claim 26, wherein said response analysis engine comprises a time-out system triggered by said event for starting a probing

Art Unit: 2437

task (*i.e.* [0068], *configured states may include some known limitations for service which are known to cause false alarms*).

**As per claim 36**, the system of claim 35, wherein said probing task verifies if any data has been detected on said network as a response to said data matched with said attack signature and, if such condition is verified:

generates an alarm in case only response signatures indicating legitimate traffic have been used by said response analysis engine (*i.e.* [0008], *generates an alarm, and [0068], limits false alarms*); or

ends the probing task in case only response signatures indicating illicit traffic or both response signatures indicating legitimate traffic and illicit traffic have been used by said response analysis engine (*i.e.* *fig 1B, and [0009]*).

**As per claim 37**, the system of claim 36, wherein, if such condition is not verified, said probing task attempts to perform a connection to a suspected attacked computer, for generating an alarm if such attempt is successful, or for ending the probing task if such attempt is unsuccessful (*i.e.* *fig 1B, and [0009]*).

**As per claim 38**, a method for detecting unauthorised use of a network, comprising the steps:

capturing data being transmitted on said network (*i.e.* [0014], *lines 31-33, monitoring process*); comparing said data with attack signatures for generating

Art Unit: 2437

an event when a match between captured data and at least one attack signature is found; and when triggered by said event;

comparing with response signatures the data being transmitted on said network as a response to said data matched with said attack signature (*i.e. [0016], matching the data stream against known misuse patterns*); and correlating the results of said comparisons with attack and response signatures for generating an alarm (*i.e. [0018], generating an alarm event*).

**As per claim 39**, the method of claim 38, wherein said data being transmitted on said network as a response to said data matched with said attack signature is captured by performing an analysis of source IP address in data packets transmitted on said network.

**As per claim 41**, the method of claim 38, wherein said data being transmitted on said network as a response to said data matched with said attack signature is captured by analysing transport level information in data packets transmitted on said network (*i.e. page 3, [0009], IP frame on TCP packets, target and destination port, for example. It is inherent that the IP address and TCP packets are included in transport layer*).

**As per claim 44**, the method of claim 43, comprising the step of generating an alarm when a match between captured data and a response

Art Unit: 2437

signature identifying illicit traffic is found (*i.e.* [0008], *generates an alarm when something suspicious is detected in traffic*).

**As per claim 47**, the method of claim 38, comprising the step of providing a time-out system, triggered by said event, for starting a probing task (*i.e.* [0068], *configured states may include some known limitations for service which are known to cause false alarms*).

**As per claim 48**, the method of claim 47, comprising the step of verifying if any data has been detected on said network as a response to said data matched with said attack signature, and, if such condition is verified:

generating an alarm in case only response signatures indicating legitimate traffic have been used engine (*i.e.* [0008], *generates an alarm, and [0068], limits false alarms*); or

ending said probing task in case only response signatures indicating illicit traffic or both response signatures indicating legitimate traffic and illicit traffic have been used (*i.e.* *fig 1B, and [0009]*).

**As per claim 49**, the method of claim 48, wherein, if such condition is not verified, said probing task attempts to perform a connection to a suspected attacked computer, for generating an alarm if such attempt is successful, or for ending the probing task if such attempt is unsuccessful (*i.e.* *fig 1B, and [0009]*).

Art Unit: 2437

**As per claim 50**, a computer program product (*i.e.* [0013], *computer program project*) capable of being loaded in the memory of at least one computer and including software code portions for performing the method of any one of claims 38 to 49 when the product is capable of being run on a computer (*i.e.* *NIDS runs on a server*).

### ***Claim Rejections - 35 USC § 103***

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

11. **Claim 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lahtinen in view of Yadav (US patent publication no. 2003/0149888 A1).**

**As per claim 29**, Lahtinen does not explicitly disclose said data being transmitted on said network as a response to said data matched with said attack signature is captured by said sniffer by analysing transport level information in data packets transmitted on said network; however, Yadav discloses data packets have been transmitted on transport level (*i.e.* page 3, [0034], *an IDS may be implemented on network transport layer so incoming packets may be monitored*).

Lahtinen and Yadav are analogous art because they are from the same field of endeavor of intrusion detection system by pattern matching.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the packets transition as described by Lahtinen and specify the packets are transmitted on transport layer as taught by Yadav because it would provide a standard way of packets exchanges at the time the invention was made.

**12. Claim 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lahtinen in view of Maher, III et al (US patent publication no. 2002/0105910) (hereinafter Marher).**

**As per claim 33**, Lahtinen does not disclose said response analysis engine comprises a counter which is incremented when a match between captured data and a response signature identifying legitimate traffic is found; however, Maher discloses the limitation (*i.e. [0045], [0047], increment or decrement counter*).

Lahtinen and Maher are analogous art because they are from the same field of endeavor of intrusion detection system by pattern matching.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the packets transition as described by Lahtinen and add an arithmetic logic unit to increment or decrement counter as taught by Maher because it would provide possibility of fine control over an objective subject.

**As per claim 34**, Lahtinen disclose when said counter reaches a predetermined value, said response analysis engine terminates without generating any alarm *(i.e. [0068], configured states may include some known limitations for service which are known to cause false alarms)*.

**As per claim 45**, Lahtinen does not discloses comprising the step of incrementing a counter when a match between captured data and a response signature identifying legitimate traffic is found; however, Maher discloses the limitation *(i.e. [0045], [0047], increment or decrement counter)*.

**As per claim 46**, Lahtinen discloses the method of claim 45, wherein said step of comparing data with response signatures is terminated when said counter reaches a predetermined value *(i.e. [0068], configured states may include some known limitations for service which are known to cause false alarms)*.

### **Examiner Notes**

Examiner has pointed out particular references contained in the prior arts of record and in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable to the limitations of the claims. It is respectfully requested from the applicant, in preparing for response, to consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the Examiner.

### ***Conclusion***

13. The following prior art made of record and not relied upon is cited to establish the level of skill in the applicant's art and those arts considered reasonably pertinent to applicant's disclosure. See **MPEP 707.05(c)**.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JING SIMS whose telephone number is (571)270-7315. The examiner can normally be reached on 7:30am-5:00pm EST, Mon-Thu.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Art Unit: 2437

/JING SIMS/

Examiner, Art Unit 2437

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2437